(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002年11月14日 (14.11.2002)

PCT

(10) 国際公開番号
WO 02/091167 A1

(51) 国際特許分類[7]: G06F 7/58

(21) 国際出願番号: PCT/JP02/03075

(22) 国際出願日: 2002年3月28日 (28.03.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-163428 2001年4月24日 (24.04.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社三技協 (SANGIKYO CORPORATION) [JP/JP]; 〒224-0053 神奈川県 横浜市 都筑区 池辺町４５０９ Kanagawa (JP). 株式会社サンテクト (SANTEKUTO CORPORATION) [JP/JP]; 〒228-0829 神奈川県 相模原市 北里２－１７－２７ Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 三田 二三夫 (MITA,Fumio) [JP/JP]; 〒228-0829 神奈川県 相模原市 北里２－１７－２７ Kanagawa (JP). 渥美 治 (ATSUMI,Osamu) [JP/JP]; 〒228-0802 神奈川県 相模原市 上鶴間２－８－３８ Kanagawa (JP).

(74) 代理人: 社本 一夫, 外 (SHAMOTO,Ichio et al.); 〒100-0004 東京都 千代田区 大手町二丁目２番１号 新大手町ビル２０６区 ユアサハラ法律特許事務所 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

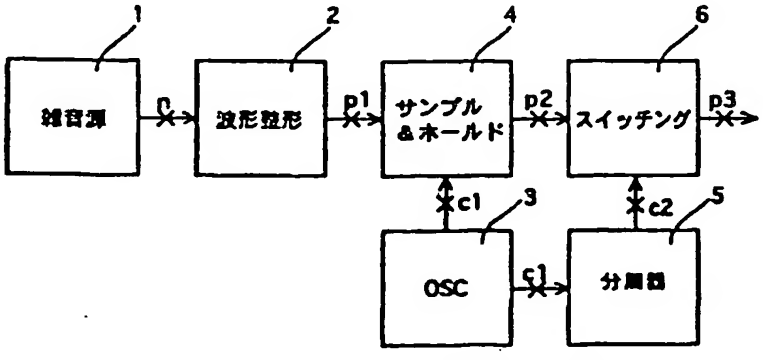
(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: RANDOM NUMBER GENERATOR

(54) 発明の名称: 乱数発生装置



(57) Abstract: A random noise n having no periodicity generated from a noise source (1) is inputted to a waveform shaper circuit (2) to generate a random pulse wave p1 which is then inputted, together with a clock c1 from an oscillator (3), to a sample & hold circuit (4) thus generating a binary pulse train p2 of constant period. The binary pulse train p2 and the clock c1 are fed to a frequency divider (5) to produce a 1/2 frequency division clock c2 which is then inputted to a switching circuit (6) in order to invert the polarity of the binary pulse train p2 every other period thus producing a smooth binary pulse train p3 where the balance of occurrence of 1/0 codes is made smooth.

[続葉有]

WO 02/091167 A1

(57) 要約:

本発明は、雑音源１が発生する周期性のないランダム雑音ｎを波形整形回路２に入力してランダムパルス波ｐ１を生成し、次に、ランダムパルス波ｐ１と発振器３のクロックｃ１をサンプル＆ホールド回路４に入力して一定周期の２値パルス列ｐ２を生成し、その２値パルス列ｐ２とクロックｃ１を分周器５で１／２に分周した１／２分周クロックｃ２をスイッチング回路６に入力して２値パルス列ｐ２の極性を１周期おきに反転させ、１／０符号の出現バランスを平滑化した平滑２値パルス列ｐ３を出力する。

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－298577
（P2000－298577A）
(43)公開日　平成12年10月24日(2000.10.24)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－104743

(22)出願日　平成11年４月13日(1999.4.13)

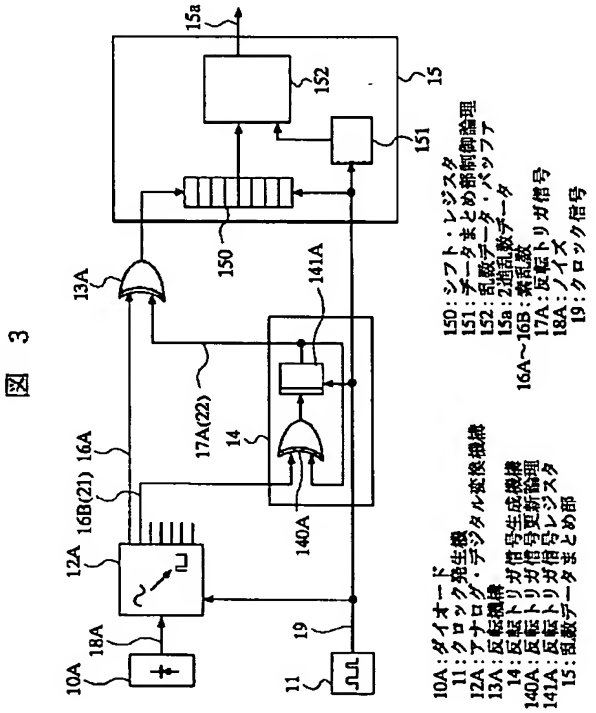
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　599050826
文部省統計数理研究所長
東京都港区南麻布４－６－７
(72)発明者　吉田　健治
神奈川県秦野市堀山下１番地　株式会社日立製作所汎用コンピュータ事業部内
(74)代理人　100080001
弁理士　筒井　大和

最終頁に続く

(54)【発明の名称】　乱数生成装置

(57)【要約】
【課題】　ランダム性のある物理現象を利用したハードウェア生成による乱数生成装置において、高速な乱数生成速度と、高い乱数性を同時に実現する。
【解決手段】　ダイオード１０Ａの出力するノイズ１８Ａを、アナログ・デジタル変換機構１２Ａでデジタル・データに変換し、デジタル・データのうちの何ビットかを素乱数１６Ａ，１６Ｂ，．．として取り出す。反転トリガ信号生成機構１４で０と１の出現比率が均等な反転トリガ信号１７Ａを生成し、反転機構１３Ａにて素乱数１６Ａとの排他的論理和をとり２進乱数データ１５ａの乱数として乱数データまとめ部１５から出力する。反転トリガ信号生成機構１４の一手段として素乱数１６Ｂを利用し、素乱数１６Ｂが１の時に直前の反転トリガ信号１７Ａの反転した値を反転トリガ信号１７Ａとして反転機構１３Ａに入力する。

図３



1

【特許請求の範囲】

【請求項１】　時間軸方向に規則性のない物理量を発生する物理量発生手段と、前記物理量を２ビット以上の第１のディジタルデータに変換するデータ変換手段と、前記第１のディジタルデータの少なくとも一部を乱数データとして外部に出力する外部出力インタフェースと、を含む乱数生成装置であって、

０と１が変化しながらほぼ同じ比率で現れる反転トリガ信号を生成する反転トリガ信号生成手段と、

前記データ変換手段と前記外部出力インタフェースとの間に設けられ、前記第１のディジタルデータの少なくとも一部のビットと、前記反転トリガ信号との排他的論理和をとり、前記第１のディジタルデータの代わりに第２のディジタルデータとして前記外部出力インタフェースに出力するデータ反転手段と、

を含むことを特徴とする乱数生成装置。

【請求項２】　請求項１記載の乱数生成装置において、前記反転トリガ信号生成手段は、任意の乱数発生手段から時系列に入力されるディジタルの乱数データと、自身の出力との排他的論理和をとり、前記反転トリガ信号として出力する反転トリガ更新論理と、前記反転トリガ更新論理から出力される前記反転トリガ信号をラッチして前記データ反転手段および前記反転トリガ更新論理に出力する反転トリガ信号ラッチ手段とを含むことを特徴とする乱数生成装置。

【請求項３】　請求項１または２記載の乱数生成装置において、

前記反転トリガ信号生成手段の前記反転トリガ更新論理に入力される前記乱数データとして、前記第１のディジタルデータの一部を用いる構成、

前記物理量発生手段および前記データ変換手段の組み合わせを、ディジタルデータを前記データ反転手段に入力する組と、前記ディジタルデータを前記乱数データとして前記反転トリガ信号生成手段の前記反転トリガ更新論理に入力する組の２系統設ける構成、

前記物理量発生手段および前記データ変換手段の組み合わせを、前記ディジタルデータを前記データ反転手段に入力する組と、前記ディジタルデータを前記乱数データとして前記反転トリガ信号生成手段の前記反転トリガ更新論理に入力する組の２系統設け、前記反転トリガ更新論理に前記乱数データとして入力される前記ディジタルデータとして、互いに他の前記ディジタルデータを用いる構成、

前記反転トリガ更新論理に入力される前記乱数データとして、ソフトウェア生成乱数を用いる構成、

のいずれかの構成を含むことを特徴とする乱数生成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、乱数生成技術に関し、特に、ハードウェアによって乱数を生成する場合における生成過程の高速化および高い乱数性の実現等に好適な乱数生成技術に関する。

2

【０００２】

【従来の技術】乱数は、様々なシミュレーションにおける不確定要素や、無作為抽出のための選択手段、暗号化技術の鍵生成などの分野で利用される。たとえば、風洞実験のシミュレーションで与える風は均質な物でなく、風向、風速、圧力などいくつものパラメータに不確定さが必要になる。また、数学の世界では、モンテカルロ法など乱数を計算に使用する。こうした乱数に、多くはソフトウェア生成の乱数が用いられている。

【０００３】しかし、ソフトウェア乱数は疑似乱数と呼ばれるように、出力した乱数列に一定の規則性があり、結果に誤った指向性が出たり、結果の収束に影響したりすることがある。

【０００４】ハードウェア生成による乱数は、乱数源にランダム性があり、時間方向に規則性の無い物理現象を選ぶことによって、ソフトウェア乱数の様な規則性を無くすことができる。たとえば、仁木直人「工学的乱数発生」統計数理研究所彙報　第２７巻　第１号　１９８０　１１５－１３１、等の文献にも記載されているように、過去のハードウェア乱数生成の乱数源に選ばれたランダム性のある物理現象には、コバルト－６０の放射線量、セシウム－１３７の崩壊によるガンマ線放射、トランジスタの熱雑音、ダイオードの熱雑音、ネオン放電管からの雑音等がある。

【０００５】乱数への加工方法として２種類の例を示す。ひとつは、前記の放射線量や、ノイズをパルス化したものを、一定時間計数した結果が偶数であるか奇数であるかで２進１桁乱数を生成する方法である。もうひとつは、ランダム性のある物理現象のうちノイズが得られるものを利用し、得られたノイズをアナログ・デジタル変換し、出力の何桁かを乱数として利用する方法である。後者の例として、特開平６－３１４１８８号公報の技術では、導線上のノイズをアナログ・デジタル変換し、乱数を生成している。

【０００６】

【発明が解決しようとする課題】２進乱数の乱数性の評価の尺度には、（１）０と１の出現する比率が等しいこと、（２）ある桁の０と１の出現する比率が、前に出現した別の桁のパターンに左右されないこと、がある。

【０００７】本明細書の中で（１）は「０と１の出現比率が等しい」、（２）は「乱数列の規則性が無い」と表現する。（２）について例を挙げると、００と続いた後の０と１の出現する比率が１：３となる場合「規則性がある」わけで、それだけ「乱数性が悪い」となる。

（１）（２）はいずれも統計的な評価のため、評価対象の母集団が大きいほど正しく評価でき、母集団が小さいケースでは常に成り立つものでは無い。

【０００８】従来の技術で説明した、一定時間におけるある物理現象を計数することによる乱数生成装置は、計数した値が充分大きくなる時間を必要とする。極端な例を挙げると、一定時間計数した結果が０から１程度だとして、ほとんどの場合０だとすると偶数と奇数の出現比率が著しく不均等なために、出力する乱数に指向性が出てしまう。たとえば１００を中心に５０から１５０の値を計数できるような、充分大きく、充分ばらつきのある値が計数できる時間を取れば、偶数と奇数の出現比率の不均衡が無視できる様になる。しかし、出現比率の差を小さくするために計数時間を大きくとれば、乱数の生成速度は反比例して遅くなる。前述した１００を中心に５０から１５０の値を計時できるような時間をとると、理論上回路の動作周波数の１／１５０以下、おそらくは１／２００から１／３００程度の乱数生成速度しか得られない。

【０００９】従来の技術で説明したもう一方の、ランダム性のあるノイズをアナログ・デジタル変換し、出力の何桁かを乱数として利用する方法では、アナログ・デジタル変換機構の回路上のくせによって各桁の０と１の出現比率が均等にならない場合が考えられる。ノイズをアナログ・デジタル変換する方法では物理現象を計数する方法に比べて、回路の動作周波数とほぼ同等の乱数生成速度を得ることができる。しかし、回路内の主にアナログ・デジタル変換機構内部の信号が０から１、１から０に変化する速さの違いやスレッショールド電圧の違いを始め、ノイズ源のダイオードから誘導される電源線、接地線、信号線へのノイズなど、回路特有のくせにより、実際のノイズの電圧値とアナログ・デジタル変換機構が出力するデジタル・データの値に誤差が生じる。たとえば、変換前のノイズがｘからｘ＋１の中間の電圧であった場合に、アナログ・デジタル変換機構の出力する結果がｘよりｘ＋１を出力する確率が多いと、出力する各桁の０と１の出現比率に偏りが生じてしまい、これを乱数とすると０と１の出現比率に偏りがある乱数になる。回路のくせは、回路を構成する素子の特性、温度、供給電＊圧、動作周波数など、様々な条件に左右され、回路の改善で偏りを無くすことは困難である。

【００１０】本発明の目的は、ハードウェアによって乱数列を生成する乱数生成技術において、高速な乱数生成速度と、乱数列に規則性が無く、均質な０と１の出現比率を同時に実現することにある。

【００１１】

【課題を解決するための手段】本発明では、物理量発生手段から得られる時間軸方向に規則性のない物理量をディジタル量に変換するアナログ・デジタル変換機構の出力するデジタル・データのあるビット（以下、素乱数と呼ぶ）を、反転トリガ信号と排他的論理和を取って乱数とする。反転トリガ信号は、０と１の出現比率が１：１となり、できるだけ規則性の無いものを生成する。この方法により、乱数として０を出力する場合に、アナログ・デジタル変換機構が０を出力している場合と１を出力している場合とどちらの場合もあり、乱数として１を出力する場合も同じくアナログ・デジタル変換機構が０を出力している場合と１を出力している場合とどちらの場合もあるため、アナログ・デジタル変換機構の回路の特有のくせが出力に与える影響を無くすことができる。

【００１２】また、反転トリガ信号に規則性がある場合にも、出力した乱数列の規則性は改善される。反転トリガ信号の規則性を、０が出現した後に０と１が出現する確率をａ：１－ａ（０＜ａ＜１）とすると、０と１の出現比率が１：１なので、１が出現した後の０と１が出現する確率は１－ａ：ａとなる。素乱数の０と１の出現比率の偏りも簡単のため、同じくａ：１－ａとして、ａの値が0.5からずれた場合、出力する乱数列の規則性にどの程度の影響が出るか計算してみる。出力する乱数列の規則性は、前記の表現と同じように０が出現した後の０と１が出現する確率をｂ：１－ｂ、１の出現した後の０と１の出現する確率を１－ｂ：ｂと表現する。すると、

【００１３】

【数１】

$$b = 4 \times a^3 - 6 \times a^2 + 3 \times a \qquad \text{【式1】}$$

【００１４】となる。実際ａが0.5近辺の値を取った場合、ｂはどうなるか計算して図７に示す。

【００１５】ａ、ｂの0.5との差分と0.5との比率を以下では、乱数の偏差と表現することとする。図７を見ると分かるように、素乱数の偏差が１％の場合で、出力した乱数の偏差は10^{-6}と非常に小さくできる。

【００１６】本発明で採用している反転トリガ信号生成機構は、反転トリガ信号生成機構に入力する素乱数が１の時に同期して反転トリガ信号を０から１又は１から０へ切り替え、素乱数が０の時は反転トリガ信号を変化させない。素乱数の乱数列には規則性が無いため、生成した反転トリガ信号は０と１の出現比率は理論上均等になる。図６は、素乱数２１とこの素乱数２１を元に生成した反転トリガ信号２２の関係の一例を信号の波形で表している。信号の波形が上にある時の信号の値が１を表し、信号の波形が下にある時の信号の値が０を表す。素乱数２１は０の出現比率が高いが、反転トリガ信号２２は０と１の出現比率はほぼ等しくなっているのがわかる。

【００１７】反転トリガ信号の規則性は、素乱数の偏差と同程度の影響がある。なぜなら、規則性の一つである０の後１になる確率、１の後０になる確率は、素乱数の１が出現する確率に等しいからである。しかし、後述する実施の形態で見てみた場合、うまく回路を構成することによって、アナログ・デジタル変換機構の出力のうち、偏差が１～２％程度の素乱数を得ることが可能であ

り、前述したように、この程度の偏差が出力の偏差に与える影響は非常に小さくできる。また、規則性が存在するソフトウェア乱数と組み合わせて乱数を生成しても、乱数性の高い乱数が得られる。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【００１９】図１は、本発明の一実施の形態である乱数生成装置の構成の一例を示す概念図である。本実施の形態の乱数生成装置は、経時的に不規則なノイズ１８Ａを発生するダイオード１０Ａ、ノイズ１８Ａを素乱数１６Ａ～１６Ｄのディジタルデータに変換するアナログ・デジタル変換機構１２Ａ、反転トリガ信号１７Ａ～１７Ｄを生成する反転トリガ信号生成機構１４、アナログ・デジタル変換機構１２Ａおよび反転トリガ信号生成機構１４にクロック信号１９を供給するクロック発生機構１１、乱数を使用する外部の任意の情報処理装置等との間のインタフェースを提供する乱数データまとめ部１５、を含んでいる。

【００２０】すなわち、ダイオード１０Ａが出力するノイズ１８Ａをアナログ・デジタル変換機構１２Ａに入力する。アナログ・デジタル変換機構１２Ａの出力する素乱数のうちの素乱数１６Ａ～１６Ｄを反転機構１３Ａ～１３Ｂのデータ入力に、反転トリガ信号生成機構１４の出力する反転トリガ信号１７Ａ～１７Ｂは、反転機構１３Ａ～１３Ｂの反転トリガ入力に接続する。反転機構の１３Ａの出力は、乱数データまとめ部１５に接続する。

【００２１】このような構成の本実施の形態の乱数生成装置の動作としては、まず、アナログ・デジタル変換機構１２Ａは、クロック信号１９に同期して、ノイズ１８Ａの電圧をデジタル・データに変換する。このデジタル・データから素乱数１６Ａ～１６Ｄを取り出す。反転機構１３Ａ～１３Ｂは、素乱数１６Ａ～１６Ｄと反転トリガ信号生成機構１４の出力する反転トリガ信号１７Ａ～１７Ｂの排他的論理和を出力し、乱数データまとめ部１５に送る。乱数データまとめ部１５は、外部からの要求でデータを取り出しやすいように加工し、２進乱数データ１５ａとして出力する。素乱数のビット数と反転機構の数は同じだが、反転トリガ信号はそれと異なっても構わない。

【００２２】図２は、前述の図１に例示された乱数生成装置のより具体的な変形例を示す概念図である。すなわち、この図２の構成例は、図１の反転トリガ信号生成機構１４の実現方法の一つを提示している。

【００２３】この図２の構成では、反転トリガ信号生成機構１４は、複数の反転トリガ信号更新論理１４０Ａ～１４０Ｂおよび反転トリガ信号レジスタ１４１Ａ～１４１Ｂを含んでいる。そして、アナログ・デジタル変換機構１２Ａの出力する素乱数のうち反転機構１３Ａ～１３Ｂに直接送られなかった素乱数１６Ｅ～１６Ｆを、それぞれ反転トリガ信号生成機構１４内の反転トリガ信号更新論理１４０Ａ～１４０Ｂに接続する。反転トリガ信号更新論理１４０Ａ～１４０Ｂの出力はそれぞれ反転トリガ信号レジスタ１４１Ａ～１４１Ｂに接続し、反転トリガ信号レジスタ１４１Ａ～１４１Ｂの出力する反転トリガ信号１７Ａ～１７Ｂは、反転機構１３Ａ～１３Ｂのいずれかの反転トリガ入力と、それぞれ反転トリガ信号更新論理１４０Ａ～１４０Ｂに接続する。

【００２４】この図２の変形例の動作としては、反転トリガ信号更新論理１４０Ａは、反転トリガ信号１７Ａと素乱数１６Ｅの排他的論理和を出力する。反転トリガ信号レジスタ１４１Ａは、クロック信号１９に同期して、保持する値を反転トリガ信号更新論理１４０Ａの出力に置き換える。反転トリガ信号更新論理１４０Ｂと反転トリガ信号１７Ｂ、素乱数１６Ｆ、反転トリガ信号レジスタ１４１Ｂの動作も同様である。このようにして、反転トリガ信号１７Ａ、１７Ｂを生成する以外は図１の説明と同様である。

【００２５】図３は、本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。この図３の構成の場合、アナログ・デジタル変換機構１２Ａは８ビット出力のものとし、アナログ・デジタル変換機構１２Ａの出力する８個の素乱数のうち１個の素乱数１６Ａを１個の反転機構１３Ａのデータ入力に、別の１個の素乱数１６Ｂを反転トリガ信号生成機構１４内の１個の反転トリガ信号更新論理１４０Ａに接続する。反転トリガ信号更新論理１４０Ａの出力は反転トリガ信号レジスタ１４１Ａに接続し、反転トリガ信号レジスタ１４１Ａの出力する反転トリガ信号１７Ａは、反転機構１３Ａの反転トリガ入力と、反転トリガ信号更新論理１４０Ａの入力側に接続する。

【００２６】反転機構１３Ａの出力は、乱数データまとめ部１５内のシフト・レジスタ１５０に接続し、シフト・レジスタ１５０の出力は、乱数データまとめ部１５内の乱数データ・バッファ１５２に接続する。乱数データまとめ部１５内のデータまとめ部制御論理１５１の出力は、乱数データ・バッファ１５２に接続する。クロック発生機構１１が出力するクロック信号１９は、アナログ・デジタル変換機構１２Ａと、反転トリガ信号レジスタ１４１Ａと、シフト・レジスタ１５０と、データまとめ部制御論理１５１に接続する。

【００２７】この図３の構成の乱数生成装置の動作としては、まず、アナログ・デジタル変換機構１２Ａは、クロック信号１９に同期して、ノイズ１８Ａの電圧を８ビットのデジタル・データに変換する。このデジタル・データから２個の素乱数１６Ａと１６Ｂを取り出す。反転トリガ信号更新論理１４０Ａは、反転トリガ信号１７Ａと素乱数１６Ｂの排他的論理和を出力する。反転トリガ信号レジスタ１４１Ａは、クロック信号１９に同期して、保持する値を反転トリガ信号更新論理１４０Ａの出

力に置き換える。反転機構１３Ａは、素乱数１６Ａと反転トリガ信号１７Ａの排他的論理和を出力し、シフト・レジスタ１５０に入力する。シフト・レジスタ１５０は、８ビットのシフト・レジスタで、クロック信号１９に同期してシフト動作と、反転機構１３Ａの出力の取り込みを行う。シフト・レジスタ１５０は、８ビット幅の出力を乱数データ・バッファ１５２に送り、データまとめ部制御論理１５１は、クロック信号１９に同期して、８サイクルに１回、乱数データ・バッファ１５２に書き込み指示を行う。乱数データ・バッファ１５２は、書き込み指示を受けた時のシフト・レジスタ１５０からのデータ（２進乱数データ１５ａ）を記憶する。また乱数データ・バッファ１５２は、外部からの読み出し要求に対して、２進乱数データ１５ａの書き出しと、書き出した２進乱数データ１５ａの消去を行う機能と、たとえばＰＣＩ等の汎用バス等に対する接続インターフェースを有し、８ビットの乱数データ（２進乱数データ１５ａ）を外部の任意の装置等に供給することができる。

【００２８】図４は本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。この図４の構成では、反転トリガ信号生成機構１４に対する素乱数の入力手段として専用のダイオード１０Ｂおよびアナログ・デジタル変換機構１２Ｂを設けた構成となっている。

【００２９】すなわち、反転機構１３Ａ～１３Ｂに接続する素乱数１６Ａ～１６Ｂに、ダイオード１０Ａが出力するノイズ１８Ａをアナログ・デジタル変換機構１２Ａがアナログ・デジタル変換した出力を用い、反転トリガ信号生成機構１４内の反転トリガ信号更新論理１４０Ａ～１４０Ｂに接続する素乱数１６Ｅ～１６Ｆに、ダイオード１０Ｂが出力するノイズ１８Ｂをアナログ・デジタル変換機構１２Ｂがアナログ・デジタル変換した出力を用いている。

【００３０】この図４の構成では、複数のダイオード１０Ａおよび１０Ｂと、アナログ・デジタル変換機構１２Ａおよび１２Ｂの組合せを２系統用意したことにより、複数の反転機構１３Ａおよび１３Ｂに入力される素乱数１６Ａおよび１６Ｂと、反転トリガ信号１７Ａおよび１７Ｂとの間の相関を無くすことが可能となり、最終的に乱数データまとめ部１５から出力される２進乱数データ１５ａにおいてより高い乱数性を実現することができる。

【００３１】図５は、図４に例示した本発明の乱数生成装置の変形例を示す概念図である。この図５の構成では、ダイオード１０Ａおよびアナログ・デジタル変換機構１２Ａと、ダイオード１０Ｂおよびアナログ・デジタル変換機構１２Ｂ、の２系列の素乱数１６Ａ、素乱数１６Ｂ、および素乱数１６Ｇ、素乱数１６Ｈ、に対して、対応した反転機構１３Ａ、１３Ｂおよび反転機構１３Ｃ、１３Ｄを設けるとともに、反転機構１３Ａ、１３Ｂおよび反転機構１３Ｃ、１３Ｄの各々に対する反転トリガ信号１７Ａおよび反転トリガ信号１７Ｂが、互いに他方のアナログ・デジタル変換機構１２Ｂおよび１２Ａから発生された素乱数１６Ｅおよび素乱数１６Ｊにてクロスして生成される構成としたものである。

【００３２】すなわち、ダイオード１０Ａが出力するノイズ１８Ａを８ビット出力のアナログ・デジタル変換機構１２Ａに入力する。ダイオード１０Ｂが出力するノイズ１８Ｂを８ビット出力のアナログ・デジタル変換機構１２Ｂに入力する。アナログ・デジタル変換機構１２Ａの出力する８個の素乱数のうち１個の素乱数１６Ａを反転機構１３Ａのデータ入力に、１個の素乱数１６Ｂを反転機構１３Ｂのデータ入力に、１個の素乱数１６Ｃを反転トリガ信号生成機構１４内の反転トリガ信号更新論理１４０Ｂに接続する。アナログ・デジタル変換機構１２Ｂの出力する８個の素乱数のうち１個の素乱数１６Ｇを反転機構１３Ｃのデータ入力に、１個の素乱数１６Ｈを反転機構１３Ｄのデータ入力に、１桁の素乱数１６Ｊを反転トリガ信号生成機構１４内の反転トリガ信号更新論理１４０Ａに接続する。反転トリガ信号更新論理１４０Ａの出力は反転トリガ信号レジスタ１４１Ａに接続し、反転トリガ信号レジスタ１４１Ａの出力する反転トリガ信号１７Ａは、反転機構１３Ａ、１３Ｂの反転トリガ入力と、反転トリガ信号更新論理１４０Ａの入力側に接続する。反転トリガ信号更新論理１４０Ｂの出力は反転トリガ信号レジスタ１４１Ｂに接続し、反転トリガ信号レジスタ１４１Ｂの出力する反転トリガ信号１７Ｂは、反転機構１３Ｃ、１３Ｄの反転トリガ入力と、反転トリガ信号更新論理１４０Ｂに接続する。反転機構の１３Ａ、１３Ｂ、１３Ｃ、１３Ｄの出力は、乱数データまとめ部１５に接続する。クロック発生機構１１が出力するクロック信号１９は、アナログ・デジタル変換機構１２Ａ、１２Ｂと、反転トリガ信号レジスタ１４１Ａ、１４１Ｂと、乱数データまとめ部１５に接続する。前述の図３の実施の形態と異なるのは、（１）ダイオードとアナログ・デジタル変換機構が２個ずつあること、（２）１個のアナログ・デジタル変換機構に対して、２個の反転機構を備え、２個の素乱数を１個ずつ、それぞれの反転機構に入力していること、（３）アナログ・デジタル変換機構１２Ａの出力する素乱数１６Ａ、１６Ｂの接続する、反転機構１３Ａ、１３Ｂに入力する反転トリガ信号１７Ａは、もう一方のアナログ・デジタル変換機構１２Ｂの出力する素乱数１６Ｊを利用して更新し、アナログ・デジタル変換機構１２Ｂの出力する素乱数１６Ｇ、１６Ｈの接続する、反転機構１３Ｃ、１３Ｄに入力する反転トリガ信号１７Ｂは、もう一方のアナログ・デジタル変換機構１２Ａの出力する素乱数１６Ｅを利用して更新していること、である。

【００３３】乱数データまとめ部１５内では図３の実施の形態と同じように、外からの読み出し要求に応答でき

るようにデータの形を整え記憶する。本実施の形態では、ダイオードから乱数データまとめ部１５の前までの回路を倍にし、利用する素乱数も倍にして乱数生成速度の性能を向上し、しかも反転トリガ信号１７Ａ、反転トリガ信号１７Ｂを更新するための素乱数１６Ｊ、１６Ｅを交換しあうことで、素乱数１６Ａ、１６Ｂおよび素乱数１６Ｇ、１６Ｈと、反転トリガ信号１７Ａ、１７Ｂを別系統の乱数源から生成するため、反転機構１３Ａ、１３Ｂおよび反転機構１３Ｃ、１３Ｄのデータ入力（素乱数１６Ａ、１６Ｂおよび素乱数１６Ｇ、１６Ｈ）、反転トリガ信号１７Ａ、１７Ｂの間の予期せぬ相関から規則性が生じることを回避している。

【００３４】なお、上述の図２～図５における乱数生成装置の構成例では、反転トリガ信号生成機構１４において反転トリガ信号１７Ａ、１７Ｂ等を生成するための素乱数は、ダイオード１０Ａ、１０Ｂおよびアナログ・デジタル変換機構１２Ａ、１２Ｂ等を用いてハードウェア的に得られた素乱数を用いているが、これに限らず、図８に例示されるように、ソフトウェア乱数生成装置３０において、たとえばM系列法、合同式法等の所望のアルゴリズムを用いたソフトウェアにて生成されたソフトウェア素乱数３０ａを、素乱数１６Ｂ、１６Ｅ、１６Ｆ、１６Ｊ、等の代わりに用いても、同様に、得られる２進乱数データ１５ａの生成速度が高速で、乱数列に規則性が無く、均質な０と１の出現比率を同時に実現することが可能になる。この場合、ソフトウェア乱数生成装置３０は、たとえば図示しないマイクロプロセッサや、乱数を生成するためのソフトウェア等が格納されるＲＯＭ、ＲＡＭ等を備えた一般的に情報処理装置で構成することができる。

【００３５】さらに、図９のフローチャートに例示されるように、反転トリガ信号生成機構１４および反転機構１３Ａ～１３Ｄ等で行われる素乱数１６Ａ、１６Ｂ、１６Ｈ、１６Ｇ等の反転処理を、当該素乱数１６Ａ～１６Ｇを利用する任意の情報処理装置の内部で、ソフトウェア的に行わせることもできる。この場合、物理現象を利用する乱数発生機構としては、本発明の上述の実施の形態で例示したダイオード１０Ａ、アナログ・デジタル変換機構１２Ａ、乱数データまとめ部１５等で構成された、素乱数１６Ａ等をそのまま外部に出力する構成の物理乱数生成装置を用いることができる。

【００３６】すなわち、任意の情報処理装置において、物理乱数生成装置から得られる素乱数１６Ａを用いるプログラムでは、前処理として、図９のフローチャートに例示された以下のような処理を行うことで乱数性の向上を達成することができる。

【００３７】すなわち、まず、物理乱数生成装置から得られた素乱数１６Ａ（２進ハードウェア乱数）を、整数変数ＨＲに格納する（ステップ２０１）。

【００３８】次に、自前のソフトウェアによる乱数発生ルーチンから２進ソフトウェア乱数を生成して整数変数ＳＲに格納する（ステップ２０２）。

【００３９】整数変数ＳＲの各ビットを指定するためのビット指標変数ｎを０に初期化する（ステップ２０３）。だだし、ＳＲ〔ｎ＝０〕はＬＳＢを示す。

【００４０】次に、ＳＲのＬＳＢ（ＳＲ〔ｎ＝０〕）を“０”との排他的論理和をとって更新する（ステップ２０４）。

【００４１】その後、ビット指標変数ｎをインクリメントして（ステップ２０５）、ビット位置がＳＲのＭＳＢを越えたか否かを判定（ステップ２０６）しながら、ＳＲのＭＳＢ方向に隣接する第ｎビットと第ｎ－１ビットとの排他的論理和をとって当該第ｎビット位置のビット値を更新する（ステップ２０７）操作を、ＭＳＢまで反復し、このステップ２０７の操作が終わったら、整数変数ＨＲに格納された２進ハードウェア乱数と、整数変数ＳＲに格納された反転操作後の２進ソフトウェア乱数との間で各ビット毎の排他的論理和をとり、結果を整数変数ＨＲに書き戻す処理（ステップ２０８）、を行う。

【００４２】これにより、整数変数ＨＲ内には、結果として、図１の乱数データまとめ部１５から得られる２進乱数データ１５ａと同様に、乱数列に規則性が無く、均質な０と１の出現比率を持つ、２進ハードウェア乱数が得られる。

【００４３】この場合には、ソフトウェア的にビット反転処理を行うため、多少、生成速度は犠牲になるが、素乱数１６Ａを供給する物理乱数生成装置は任意のものを用いることができ、物理乱数を利用する情報処理装置のソフトウェアの側のわずかな変更で、高い乱数性を持つ物理乱数を使用できるようになる、という利点がある。また、生成速度の点も、物理乱数を利用する情報処理装置の実行速度が改善されれば問題にならなくなり、乱数生成の高速性の要求も満たされる。

【００４４】以上説明したように、本実施の形態の乱数生成装置では、ハードウェアによる高速な生成速度の乱数生成処理において、０と１の出現比率については均等にでき、素乱数の偏差が最終的に出力される乱数の規則性へ与える影響を少なくすることができる。図７で示したとおり、乱数列の規則性の偏りは、素乱数の０と１の出現比率の偏りが２％の場合で10^{-5}以下、１％で10^{-6}に改善することができる。

【００４５】本発明の特許請求の範囲に記載された以外のの特徴を列挙すれば以下の通りである。

【００４６】＜１＞　ノイズ源としてのダイオードと、アナログ・デジタル変換機構と、乱数データまとめ部と、クロック発生機構を有し、クロック発生機構が発生するクロック信号を、前記アナログ・デジタル変換機構に接続し、前記ダイオードに逆バイアスをかけた場合のツェナー降伏領域もしくはアバランシェ領域で発生するノイズの電圧を、前記アナログ・デジタル変換機構で前

記クロックに同期してｎビット（ｎ＞１）のデジタル・データに変換し、該デジタル・データのうちｍビット（１≦ｍ≦ｎ）を乱数データまとめ部で乱数として利用できる形にまとめる乱数生成装置において、データ入力と反転トリガ入力の２個の入力を持つｍ個の反転機構と、反転トリガ信号生成機構を備え、該反転トリガ信号生成機構は、０と１が変化しながらほぼ同じ比率で現れる反転トリガ信号をｓ個（１≦ｓ≦ｍ）生成し、該ｓ個の反転トリガ信号を、合計ｍ個全ての前記反転機構の反転トリガ入力に１対１もしくは１対多で接続し、前記乱数データまとめ部に送られる直前のｍビットのデジタル・データを該ｍ個の反転機構のデータ入力に１対１で接続し、該ｍ個の反転機構はデータ入力と反転トリガ入力の排他的論理和を出力し、該出力を、前記アナログ・デジタル変換機構が出力したｍ桁のデジタル・データの代わりに前記乱数データまとめ部に送ることを特徴とする乱数生成装置。

【００４７】＜２＞　反転トリガ信号を保持するｓ個の反転トリガ信号レジスタと、ｓ個の反転トリガ信号更新論理を有し、前記アナログ・デジタル変換機構の出力するデジタル・データのうちｓビットをｓ個の該反転トリガ信号更新論理全てに１対１で接続し、該反転トリガ信号更新論理は対応する反転トリガ信号レジスタが保持する反転トリガ信号と前記入力されたデジタル・データとの排他的論理和を出力し、前記反転トリガ信号レジスタに前記クロックを接続し、該反転トリガ信号レジスタが保持している反転トリガ信号を、クロックに同期して前記反転トリガ信号更新論理の出力に置き換え、該反転トリガ信号レジスタの保持している反転トリガ信号を出力することを特徴とする反転トリガ信号生成機構を備える項目＜１＞記載の乱数生成装置。

【００４８】＜３＞　プログラム生成乱数を前記反転トリガ信号として出力する反転トリガ信号生成機構を有する、項目＜１＞記載の乱数生成装置。

【００４９】＜４＞　前記ダイオードと前記アナログ・デジタル変換機構の組み合わせを、前記反転機構のデータ入力に接続するものと、前記反転トリガ信号更新論理に接続するものを独立して２系統用意することを特徴とする項目＜２＞記載の乱数生成装置。

【００５０】＜５＞　前記ダイオードと前記アナログ・デジタル変換機構と反転機構の組み合わせを２系統有し、該反転機構の出力を別の反転機構のデータ入力と反転トリガ入力に接続することを特徴とする項目＜１＞記載の乱数生成装置。

【００５１】＜６＞　時間軸方向に不規則な物理量から２値の素乱数を生成するステップと、０と１が変化しながらほぼ同じ比率で現れる反転トリガ信号を生成するステップと、前記素乱数と前記反転トリガ信号との排他的論理和をとって２進乱数として出力するステップと、を含むことを特徴とする乱数生成方法。

【００５２】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００５３】たとえば、物理量発生手段としては、上述の実施の形態に例示したダイオードに限らず、時間軸方向に不規則な物理量を出力する一般の機器を広く用いることができる。

【００５４】

【発明の効果】本発明の乱数生成装置によれば、ハードウェアによって乱数列を生成する乱数生成技術において、高速な乱数生成速度と、乱数列に規則性が無く、均質な０と１の出現比率を同時に実現することができる、という効果が得られる。

【図面の簡単な説明】

【図１】本発明の一実施の形態である乱数生成装置の構成の一例を示す概念図である。

【図２】図１に例示された乱数生成装置のより具体的な変形例を示す概念図である。

【図３】本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。

【図４】本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。

【図５】図４に例示した本発明の乱数生成装置の変形例を示す概念図である。

【図６】素乱数と、この素乱数を元に生成した反転トリガ信号の関係の一例を信号の波形で表した線図である。

【図７】本発明の一実施の形態である乱数生成装置の作用の一例を表形式で例示した説明図である。

【図８】本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。

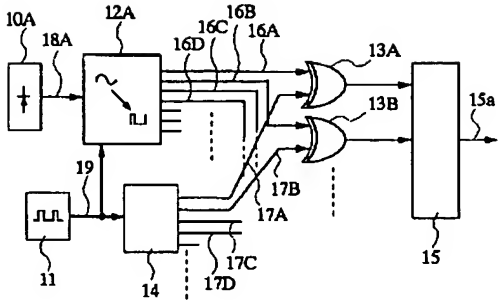
【図９】本発明の乱数生成技術をソフトウェアにて行わせる場合の一例を示すフローチャートである。

【符号の説明】

１０Ａ，１０Ｂ…ダイオード、１１…クロック発生機構、１２Ａ，１２Ｂ…アナログ・デジタル変換機構、１３Ａ～１３Ｄ…反転機構、１４…反転トリガ信号生成機構、１５…乱数データまとめ部、１５ａ…２進乱数データ、１６Ａ～１６Ｊ…素乱数、１７Ａ～１７Ｄ…反転トリガ信号、１８Ａ，１８Ｂ…ノイズ、１９…クロック信号、２１…素乱数、２２…反転トリガ信号、３０…ソフトウェア乱数生成装置、３０ａ…ソフトウェア素乱数、１４０Ａ～１４０Ｂ…反転トリガ信号更新論理、１４１Ａ～１４１Ｂ…反転トリガ信号レジスタ、１５０…シフト・レジスタ、１５１…データまとめ部制御論理、１５２…乱数データ・バッファ。

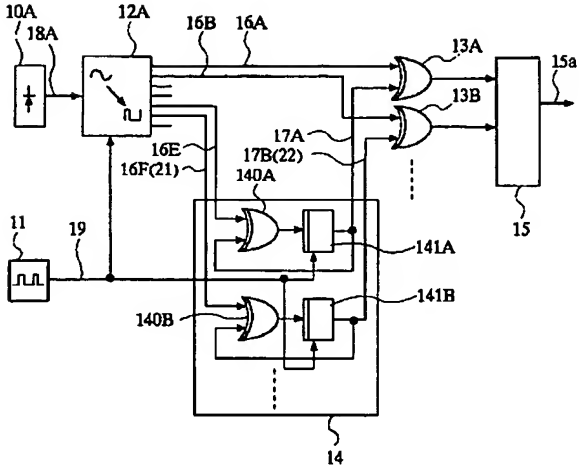
【図１】

図 1



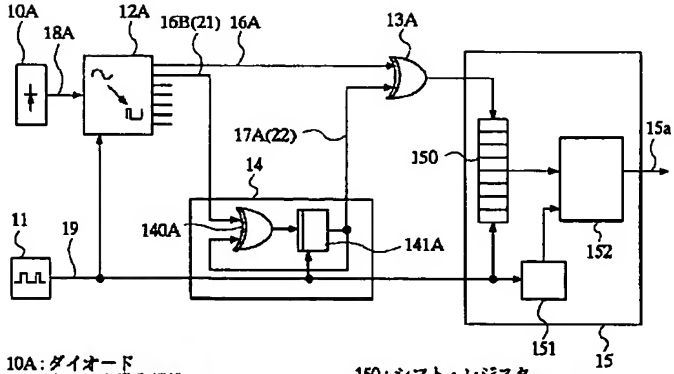
【図２】

図 2



【図３】

図 3



10A：ダイオード
11：クロック発生機構
12A：アナログ・デジタル変換機構
13A：反転機構
14：反転トリガ信号生成機構
140A：反転トリガ信号更新論理
141A：反転トリガ信号レジスタ
15：乱数データまとめ部
150：シフト・レジスタ
151：データまとめ部制御論理
152：乱数データ・バッファ
15a：2進乱数データ
16A～16B：素乱数
17A：反転トリガ信号
18A：ノイズ
19：クロック信号

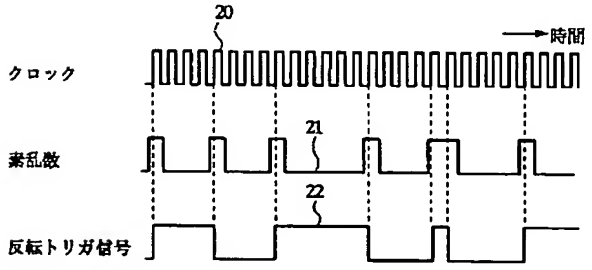
【図７】

図 7

a	b
0.6	0.504
0.55	0.5005
0.54	0.500256
0.53	0.500108
0.52	0.500032
0.51	0.500004
0.505	0.5000005
0.5	0.5

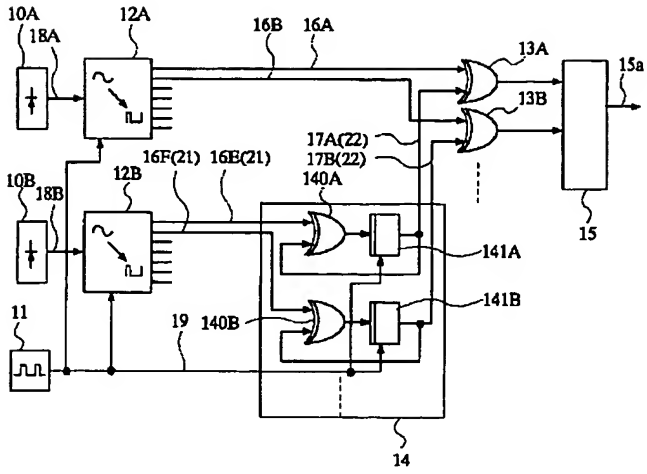
【図６】

図 6



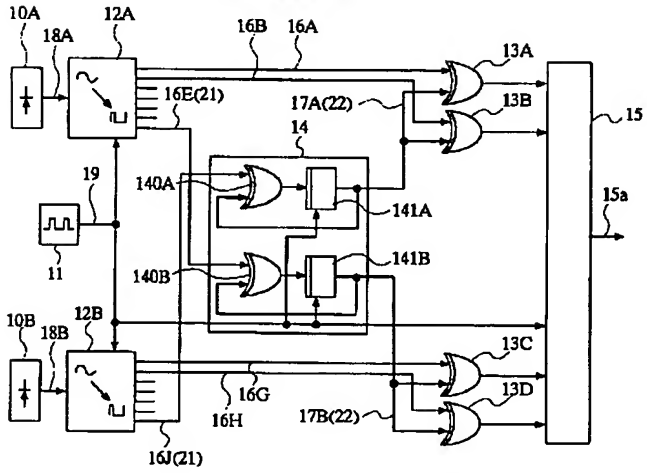
【図４】

図 4



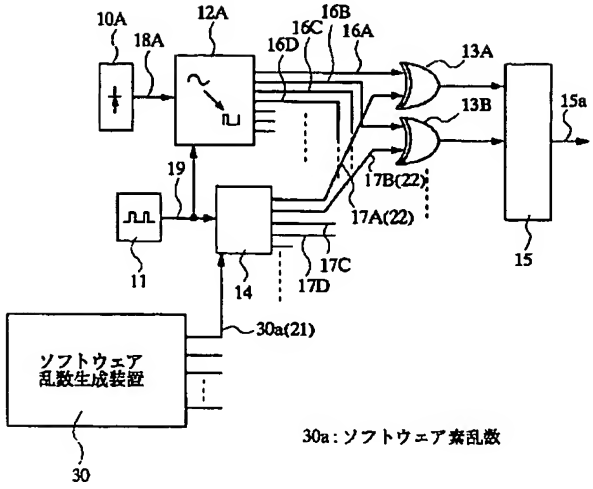
【図５】

図 5



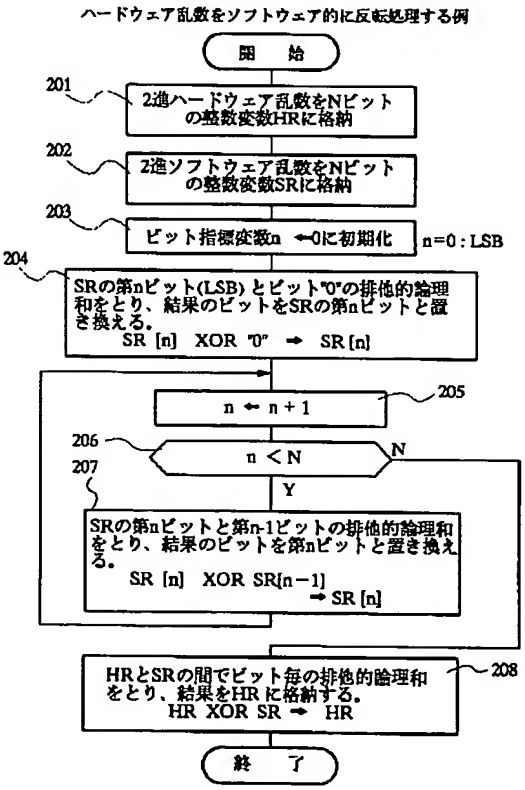
【図８】

図 8



【図９】

図 9



フロントページの続き

(72)発明者　田村　義保
東京都港区南麻布４－６－７　統計数理研究所内

(72)発明者　泰地　真弘人
東京都港区南麻布４－６－７　統計数理研究所内